What is claimed is:

1(currently amended). A method for ~~providing a fair exchange of user information by encoding said information with a hidden value~~ **fairly exchanging a hidden value of a first user for a hidden value of a second user, by a series of exchanges between the first user and the second user leading up to completing said hidden values,** comprising the ~~step~~ **steps** of:

~~selecting said hidden value as one of~~ **establishing a modulus and a modular function known to the first user and known to the second user, said modular function iteratively producing** a plurality of sequence values **wherein each said sequence value is related, according to said modular function, to a next previous sequence value**, **whereby conformance to the modular function can be determined for adjacent ones of the plurality of sequence values;**

establishing a total number of iterations over which the sequence values will be exchanged between the first user and the second user;

~~wherein difference values between adjacent ones of said sequence values are symmetrically distributed about one of said values of a known order~~

iteratively exchanging the sequence values of the first and second users, progressing in a predetermined order toward an end of said sequence values;

completing the exchange provided that the total number of iterations are completed, and terminating the exchange if the total number of iterations are not completed.

Claim 2 is canceled.

3(currently amended). The method **of** ~~as recited in~~ claim 1, wherein said plurality of values are determined ~~in accordance with~~ **according to the modular function by** a root value and a modulus value.

4(currently amended). The method **of** ~~as recited in~~ claim 1, wherein said sequence values are determined **over a known order equal to the total number of iterations, wherein each said sequence value is a result of the modular function applied to a next previous sequence value, raised to a power related to a difference in position between said sequence value and a respective beginning and end of the order** ~~as: 12 (g 2 2 i) i = 0 K mod (N) ; (g 2 ((2 K + 1) - (2 K - n))) n = 1 K mod (N) ; where K is a known order; N is a modulus value; and g is a root value~~.

Claim 5 is canceled.

6(currently amended). The method **of** ~~as recited in~~ claim 4, wherein said modulus value is **a product of** ~~selected from the group consisting of~~ Blum integers ~~in the form of N=p.sub.1p.sub.2~~.

7(currently amended). The method **of** ~~as recited in~~ claim 6, wherein said Blum integers **comprise related** ~~are selected from the group satisfying: p.sub.1=2 q.sub.1+1; and p.sub.2=2 q.sub.2+1 wherein q.sub.1 and q.sub.2 are~~ prime numbers.

Claim 8 is canceled.

9(currently amended). The method **of** ~~as recited in~~ claim 1, wherein said hidden value is ~~selected as~~ a value immediately preceding a last value of said sequence.

10(currently amended). The method **of** ~~as recited in~~ claim 1, wherein said ~~order value of known order~~ **number of iterations** is at least 80.

Claims 11 – 22 are canceled.

23(currently amended). A system for exchanging user information over a network comprising:

at least one programmed ~~[a]~~ processor ~~in communication with~~ **coupled to** a memory **and arranged for conducting a fair exchange of a hidden value of a first user for a hidden value of a second user, by a series of exchanges between the first user and the second user leading up to completing said hidden values;**

establishing a modulus and a modular function known to the first user and known to the second user, said modular function iteratively producing a plurality of sequence values wherein each said sequence value is related, according to said modular function, to a next previous sequence value, whereby conformance to the modular function can be determined for adjacent ones of the plurality of sequence values;

establishing a total number of iterations over which the sequence values will be exchanged between the first user and the second user,

iteratively exchanging the sequence values of the first and second users, progressing toward an end of said sequence values;

completing the exchange provided that the total number of iterations are completed, and terminating the exchange if the total number of iterations are not completed.

~~, said processor operable to execute for: transmitting over said network said user information encoded in association with a hidden value selected as one of a plurality of values distributed in a sequence wherein a difference between adjacent ones of said values increases and decreases symmetrically about one of said values of a known order; transmitting over said network a first set of said values, and a last value in said sequence, wherein said values in said first set have increasing differences between adjacent ones of said values; and transmitting, individually said remaining values.~~

24(currently amended). The system **of** ~~as recited in~~ claim 23, **further comprising a further processor and** wherein said processor **and said further processor exchange said sequence values on behalf of the first and second users, respectively** ~~is further operable to execute code for transmitting said remaining values in response to a received information~~.

25(currently amended). The system **of** ~~as recited in~~ claim 23, wherein said processor ~~is further operable to execute code for transmitting said remaining values~~ **is operable to effect the series of exchanges** on a timed-basis.

Claims 26-29 are canceled.